UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

SHAVONNE DIGGS, on behalf of herself and all others similarly situated, Plaintiff, v. **DISA GLOBAL SOLUTIONS, INC.,** Defendant.	Case No. 4:25-cv-00878 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Shavonne Diggs ("Plaintiff"), individually and on behalf of all similarly situated persons, allege the following against DISA Global Solutions, Inc. ("DISA" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against DISA for its failure to properly secure and safeguard Plaintiff's and other similarly situated persons' names, Social Security numbers, driver's license numbers, other government identification numbers, and financial account information (the "Private Information") from hackers.

2. DISA, based in Houston Texas, is a third-party administrator of worker background checks and drug and alcohol testing for employers that serves more than 55,000 customers (hereinafter, the "Clients" or "Defendant's Clients") across the United States and Canada.

3. On or about February 24, 2025, DISA filed official notice of a hacking incident with the Office of the Maine Attorney General.

4. On or around the same day, DISA also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident (the "Notice").

5. Based on the Notice filed by the company, on April 22, 2024, DISA detected unusual activity on some of its computer systems. In response, the company initiated an investigation. The DISA investigation revealed that between February 9, 2024 and April 22, 2024, an unauthorized party had access to certain company files containing the Private Information that DISA stored on behalf of its Clients (the "Data Breach"). Yet, DISA waited ten (10) months to notify its Clients and the public that they were at risk.

6. As a result of this delayed response, Plaintiff and "Class Members" (defined below) had no idea for *ten months* that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, Social Security numbers, driver's license numbers, other government identification numbers, and financial account information that DISA collected and maintained on behalf of its Clients' employees.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining

driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by DISA that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address DISA's inadequate safeguarding of Class Members' Private Information that it collected and maintained on behalf of its Clients, and its failure to provide timely and adequate notice to its Clients and their affected employees, such as Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to DISA, and thus DISA was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, DISA and its employees failed to properly monitor and to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had DISA properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of DISA's negligent conduct as the Private Information that DISA collected and maintained on behalf of its Clients is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of herself and the Class, assert claims for negligence, negligence *per se*, breach of third party beneficiary contract, invasion of privacy/intrusion upon seclusion, and unjust enrichment.

II. PARTIES

17. Plaintiff Shavonne Diggs is, and at all times mentioned herein was, an individual citizen of the State of Louisiana.

18. Defendant DISA Global Solutions, Inc. is an employee screening company incorporated in Delaware with its principal place of business at 12600 Northborough Drive, Suite 300, Houston, TX 77067. The registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from DISA. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A). Defendant is a citizen of Texas.

20. This Court has jurisdiction over DISA because DISA operates in and/or is incorporated and has its principal place of business in the Houston Division of the Southern District of Texas.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in the Houston Division of the Southern District of Texas and DISA has harmed Class Members residing in the Houston Division of the Southern District of Texas.

IV. FACTUAL ALLEGATIONS

A. *DISA's Business and Collection of Plaintiff's and Class Members' Private Information*

22. DISA is a is a provider of employee screening, compliance, and safety solutions for businesses across various industries. Founded in 1986, DISA is one of the largest third-party administrator companies in the industry, serving more than 55,000 companies and millions of drug tests and background checks. DISA employs more than 1,200 people and generates approximately $280 million in annual revenue.

23. As a condition of receiving screening services, DISA requires that its Clients entrust it with highly sensitive personal information belonging to their employees. In the ordinary course of receiving employment from DISA's Clients, Plaintiff and Class Members were required to provide their Private Information to Defendant.

24. DISA uses this information, *inter alia*, to provide background checks and provide drug screenings.

25. In its privacy policy, DISA promises its Clients and the public that it will not share this Private Information with third parties:

> "DISA respects the privacy of the individuals and clients who are the subjects of DISA Services, including but not limited to background checks. DISA will collect,

store, and use confidential information following best practices and also in compliance with applicable law, including the FCRA." [1]

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, DISA assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

B. ***The Data Breach and DISA's Inadequate Notice to Plaintiff and Class Members***

27. According to Defendant's Notice, it learned of unauthorized access to its computer systems on Aprill 22, 2024, with such unauthorized access having taken place between February 9, 2024 and April 22, 2024.

28. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, Social Security numbers, driver's license numbers, other government ID numbers, financial account information, relating to its Clients' employees.

29. On or about February 21, 2025, roughly over ten months after DISA learned that the Class's Private Information was first accessed by cybercriminals, DISA finally began to notify its Clients and Class Members that its investigation determined that their Private Information was involved.

30. DISA delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "Data Incident."

31. Omitted from the Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does

[1] https://disa.com/privacy-policy (last visited on Feb. 27, 2025).

not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

32. Thus, DISA's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

33. In addition, the Notice offers no substantive steps to help victims like Plaintiff and Class Members to protect themselves other than providing one year of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiff and Class Members now face as a result of the Data Breach.

34. DISA had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members in its own privacy policy to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Plaintiff and Class Members provided their Private Information to DISA, either directly or as a result of their employment with DISA's Clients, with the reasonable expectation and mutual understanding that DISA would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

36. DISA's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

37. DISA knew or should have known that its electronic records would be targeted by cybercriminals.

C. *DISA Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses in Possession of Private Information are Particularly Susceptible.*

38. DISA's negligence, including its gross negligence, in failing to safeguard Plaintiff's and Class Members' Private Information is particularly stark, considering the highly public increase of cybercrime similar to the hacking incident that resulted in the Data Breach.

39. Data thieves regularly target entities like DISA due to the highly sensitive information they maintain. DISA knew and understood that Plaintiff's and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

40. According to the Identity Theft Resource Center's 2023 Data Breach Report, the overall number of publicly reported data compromises in 2023 increased more than 72-percent over the previous high-water mark and 78-percent over 2022.[2]

41. Moreover, third-party vendors like DISA are an especially common target for hackers. In 2023, approximately 29-percent of all data breaches resulted from a "third-party attack vector" and, as much data breach reporting does not specify the attack vector, "the actual percentage of breaches occurring via third parties was probably higher."[3]

42. Despite the prevalence of public announcements of data breach and data security compromises, DISA failed to take appropriate steps to protect Plaintiff's and Class Members' Private Information from being compromised in this Data Breach.

43. As a national service provider in possession of millions of customers' Private Information, DISA knew, or should have known, the importance of safeguarding the Private

---

[2] *2023 Annual Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024), *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last visited on Feb. 27, 2025).

[3] *Global Third-Party Cybersecurity Breaches*, SECURITYSCORECARD (2024), *available online at*: https://securityscorecard.com/reports/third-party-cyber-risk/ (last visited on Feb. 27, 2025).

Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences they would suffer if DISA's data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to the unauthorized exposure of their Private Information to criminal actors. Nevertheless, DISA failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

44. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

45. DISA was, or should have been, fully aware of the unique type and the significant volume of data on DISA's network server(s) and systems and the significant number of individuals who would be harmed by the exposure of the unencrypted data.

46. Plaintiff and Class Members were the foreseeable and probable victims of DISA's inadequate security practices and procedures. DISA knew or should have known of the inherent risks in collecting and storing the Private Information and the critical importance of providing adequate security for that data, particularly due to the highly public trend of data breach incidents in recent years.

D. *DISA Failed to Comply with FTC Guidelines*

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in

violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

48. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[4] The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

49. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, and monitor their networks for suspicious activity.

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[4] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on Feb. 27, 2025).

51. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like DISA here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

52. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like DISA of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of DISA's duty in this regard.

53. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[5]

54. As evidenced by the Data Breach, DISA failed to properly implement basic data security practices. DISA's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

[5] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on Feb. 27, 2025).

55. DISA was at all times fully aware of its obligation to protect the Private Information of its Clients' employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. *DISA Failed to Comply with Industry Standards*

56. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

57. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[6]

58. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.
d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.

[6] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Feb. 27, 2025).

f. Have formal policies for safely disposing of electronic files and old devices.
g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

59. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[7]

60. Upon information and belief Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of one or more of the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the

[7] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Feb. 27, 2025).

Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

F. *DISA Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information*

61. In addition to its obligations under federal and state laws, DISA owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. DISA owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

62. DISA breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. DISA's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect the Private Information in its possession

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of the Private Information in its possession;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

63. DISA negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

64. Had DISA remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

65. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

G. *DISA Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft*

66. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data. Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment.

67. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to

monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

68. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

69. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

70. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

71. One such example of this is the development of "Fullz" packages.

72. Cybercriminals can cross-reference two sources of the Private Information

compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

73. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

74. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[8] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

75. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud,

[8] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Feb. 27, 2025).

to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

76. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

77. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[9] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

78. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit card number can

[9] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. DEP'T OF JUSTICE (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited on Feb. 27, 2025).

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited on Feb. 27, 2025).

sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[11]

79. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[12]

80. The Dark Web Price Index of 2023, published by PrivacyAffairs[13] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	**Avg. Price USD (2022)**
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

81. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

---

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web (last visited on Feb. 27, 2025).

[12] *See Dark Web Price Index: The Cost of Email Data,* MAGICSPAM, https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Feb. 27, 2025).

[13] *See Dark Web Price Index 2023*, PRIVACY AFFAIRS, https://www.privacyaffairs.com/dark-web-price-index-2023/ (last visited on Feb. 27, 2025).

82. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including DISA collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[14]

83. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[15]

84. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

85. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

86. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

---

[14] *See Privacy Policy*, ROBINHOOD, https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Feb. 27, 2025).

[15] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

87. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[16] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[17]

88. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[18]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

89. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

---

[16] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on Feb. 27, 2025).

[17] *Id* at pp 21-25.

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on Feb. 27, 2025).

90. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. *Plaintiff's and Class Members' Damages*

Plaintiff Shavonne Diggs' Experience

91. Upon information and belief, one of DISA's Clients entrusted Defendant with its employees Private Information, including the Private Information of Plaintiff Diggs.

92. Plaintiff Diggs received the Notice informing her that her Private Information had been involved during the Data Breach.

93. The Notice offered Plaintiff Diggs only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Diggs will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

94. Plaintiff Diggs suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

95. Plaintiff Diggs would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard the Private Information in its possession from theft, or that its systems were subject to a data breach.

96. Plaintiff Diggs suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

97. Plaintiff Diggs suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff

Diggs entrusted to Defendant for the purpose of receiving employment from Defendant's Client and which was compromised in, and as a result of, the Data Breach.

98. Plaintiff Diggs suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

99. Plaintiff Diggs has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

100. As a result of the Data Breach, Plaintiff Diggs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Diggs has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

101. As a result of the Data Breach, Plaintiff Diggs has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Diggs is very concerned about this

increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

102. Plaintiff Diggs also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Diggs; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

103. As a result of the Data Breach, Plaintiff Diggs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

104. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

105. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive services from Defendant's Clients.

106. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

107. As a direct and proximate result of DISA's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

108. Further, as a direct and proximate result of DISA's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

109. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

110. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

111. Additionally, as a direct and proximate result of DISA's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

112. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

113. Additionally, Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry

was worth roughly $200 billion.[19] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[20]

114. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

115. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

---

[19] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited on Feb. 27, 2025)

[20] *Frequently Asked Questions,* NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Feb. 27, 2025).

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones; and

h. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

116. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of DISA, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

117. As a direct and proximate result of DISA's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

118. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

119. Specifically, Plaintiff proposes the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

> All individuals in the United States who had Private Information impacted as a result of the Data Breach, including all who were sent a notice of the Data Breach.

120. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

121. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as the addition of any subclasses, before the Court determines whether certification is appropriate.

122. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

123. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 3.3 million of DISA Clients' employees whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through DISA's records, DISA's Clients' records, Class Members' records, publication notice, self-identification, and other means.

124. **Commonality.** There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether DISA engaged in the conduct alleged herein;

b. When DISA learned of the Data Breach;

c. Whether DISA's response to the Data Breach was adequate;

d. Whether DISA unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether DISA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether DISA's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether DISA's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether DISA owed a duty to Class Members to safeguard their Private Information;

i. Whether DISA breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether DISA had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

l. Whether DISA breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether DISA knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of DISA's misconduct;

o. Whether DISA's conduct was negligent;

p. Whether DISA's conduct was *per se* negligent;

q. Whether DISA was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

125. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

126. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

127. **Predominance.** DISA has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from DISA's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

128. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for DISA. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

129. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). DISA has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

130. Finally, all members of the proposed Class are readily ascertainable. DISA has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by DISA.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

131. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

132. DISA knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

133. DISA's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

134. DISA knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. DISA was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

135. DISA owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. DISA's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect the Private Information in its possession it using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

136. DISA's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

137. DISA's duty also arose because Defendant was bound by industry standards to protect the confidential Private Information entrusted to it.

138. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and DISA owed them a duty of care to not subject them to an unreasonable risk of harm.

139. DISA, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within DISA's possession.

140. DISA, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

141. DISA, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

142. DISA breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

143. DISA acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

144. DISA had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust DISA with their Private Information was predicated on the understanding that DISA would take adequate security precautions. Moreover, only DISA had the ability to protect its systems (and the Private Information that it stored on them) from attack.

145. DISA's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

146. DISA's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

147. As a result of DISA's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

148. DISA also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

149. As a direct and proximate result of DISA's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

150. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

151. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

152. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring DISA to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class)

153. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

154. Pursuant to Section 5 of the FTCA, DISA had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

155. DISA breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

156. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

157. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of DISA's duty in this regard.

158. DISA violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

159. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to DISA's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

160. DISA's violations of the FTCA constitute negligence *per se*.

161. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to DISA's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

162. As a direct and proximate result of DISA's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the uncompensated lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

163. DISA breached its duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

164. As a direct and proximate result of DISA's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

165. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring DISA to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

166. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

167. Defendant entered into contracts, written or implied, with its Clients to perform services that include, but are not limited to, providing employment screening services. Upon information and belief, these contracts are virtually identical between and among Defendant and

its Clients around the country whose employees, including Plaintiff and Class Members, were affected by the Data Breach.

168. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class.

169. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its Clients. Defendant knew that if it were to breach these contracts with its Clients, its Clients' employees—Plaintiff and Class Members—would be harmed.

170. Defendant breached the contracts it entered into with its Clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

171. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

172. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
INTRUSION UPON SECLUSION / INVASION OF PRIVACY
(On behalf of Plaintiff and the Nationwide Class)

173. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

174. Plaintiff and Class Members maintain a privacy interest in their Private Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

175. Plaintiff and Class Members' Private Information was contained, stored, and managed electronically in DISA's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities were only shared with DISA for the limited purpose of obtaining and paying for the services of Defendant and/or its Clients.

176. Additionally, Plaintiff's and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information for fraud, identity theft, and other crimes without the victims' knowledge and consent.

177. DISA's disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Private Information is offensive. DISA's disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties permitted the physical and electronic intrusion into private quarters where Plaintiff's and Class Members' Private Information was stored.

178. Plaintiff and Class Members have been damaged by DISA's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

179. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

180. This Count is pleaded in the alternative to Count III above.

181. Plaintiff and Class Members conferred a benefit on DISA by permitting their employer to turn over their Private Information to Defendant. Moreover, upon information and belief, Plaintiff alleges that payments made by DISA's Clients to DISA included payment for cybersecurity protection to protect Plaintiff's and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiff and Class Members in the form of elevated prices charged by DISA's Clients for their employment screening services. Plaintiff and Class Members did not receive such protection.

182. Upon information and belief, DISA funds its data security measures entirely from its general revenue, including from payments made to it by its Clients on behalf of Plaintiff and Class Members.

183. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to DISA.

184. DISA has retained the benefits of its unlawful conduct, including the amounts of payment indirectly received from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

185. DISA knew that Plaintiff and Class Members conferred a benefit upon it, which DISA accepted. DISA profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

186. If Plaintiff and Class Members had known that DISA had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

187. Due to DISA's conduct alleged herein, it would be unjust and inequitable under the circumstances for DISA to be permitted to retain the benefit of its wrongful conduct.

188. As a direct and proximate result of DISA's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in DISA's possession and is subject to further unauthorized disclosures so long as DISA fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

189. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from DISA and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by DISA from its wrongful conduct. This can be accomplished by establishing a

constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

190. Plaintiff and Class Members may not have an adequate remedy at law against DISA, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing DISA to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring DISA to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: February 27, 2025

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
S.D. Tex. Bar No. 30973
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214-744-3000 / 214-744-3015 (fax)
jkendall@kendalllawgroup.com

Tyler J. Bean (*pro hac vice* forthcoming)
Neil P. Williams (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com
E: nwilliams@sirillp.com

Attorneys for Plaintiff and the Putative Class